LISTING OF THE CLAIMS

1. (Previously Amended) A method for reducing the boot time of a Trusted Computing Performance Alliance (TCPA) based computing system comprising the steps of:

resetting said TCPA computing system;

executing a boot block code comprising a Core Root of Trust for Measurement (CRTM);

reading bits in a register of a flash memory storing said boot block code, wherein said bits in said register indicate whether segments of said flash memory have been updated; and

obtaining one or more measurement values from a table storing hashed values from a previous measurement of a Power On Self Test (POST) Basic Input/Output System (BIOS) if one or more of said bits read in said register indicate one or more of said segments of said flash memory storing said POST BIOS have not been updated.

2. (Original) The method as recited in claim 1 further comprising the step of:

transmitting said obtained measurement values to a Trusted Platform Module.

3. (Original) The method as recited in claim 2 further comprising the steps of:

setting a control bit in said register so no other device can set said bits read in said register; and

executing said POST BIOS.

4. (Original) The method as recited in claim 1 further comprising the steps of:

performing a measurement of a segment of said flash memory storing said POST BIOS which is indicated by a bit in said register as having been updated;

performing a look-up in said table of a previous measurement of said segment updated of said flash memory storing said POST BIOS; and

comparing said measured value with said looked-up value in said table.

5. (Original) The method as recited in claim 4 further comprising the step of:

taking appropriate security measures if said measured value is not equal with said looked-up value in said table.

6. (Original) The method as recited in claim 4 further comprising the step of:

resetting said bit in said register to indicate that said segment of said flash memory is validated if said measured value is equal with said looked-up value in said table.

7. (Original) The method as recited in 6 further comprising the step of:

transmitting said measured value of said segment of said flash memory updated and said obtained measurement values of one of more of said segments of said flash memory storing said POST BIOS that have not been updated to a Trusted Platform Module.

Claims 8-21 (Cancelled)